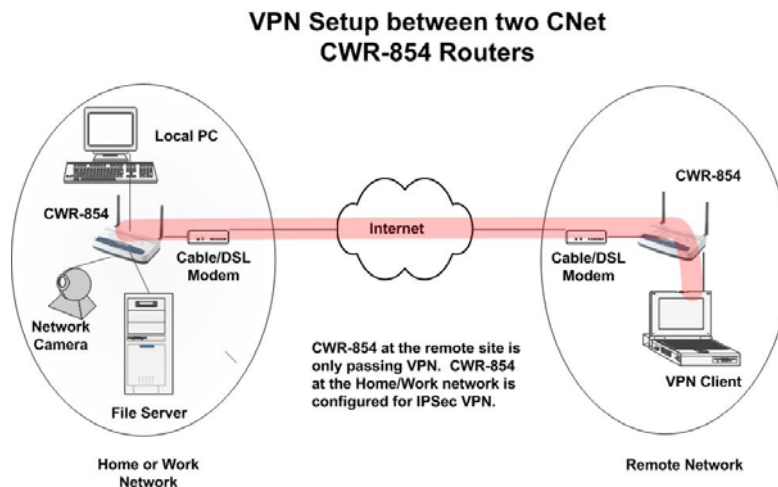
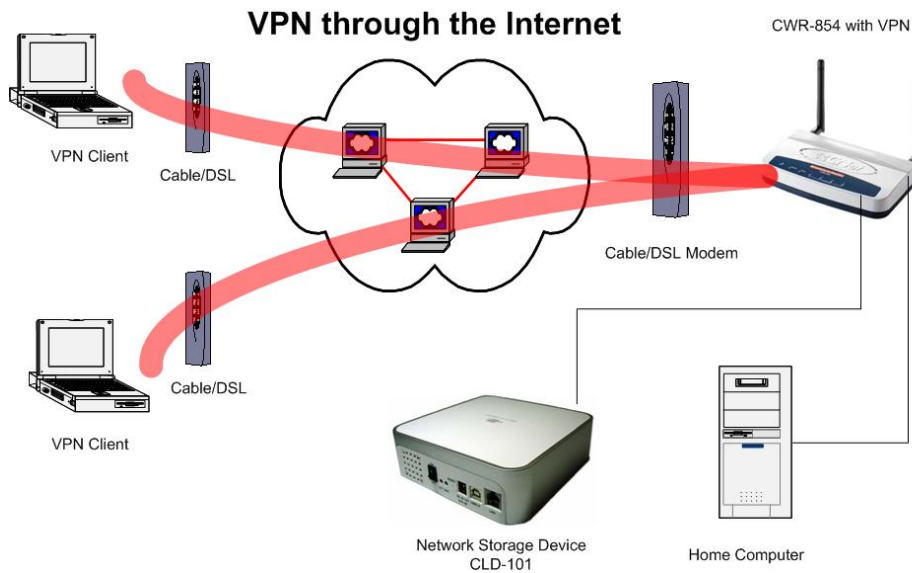


# VPN Setup for CNet's CWR-854 802.11g Wireless Router

The instructions below are for getting an IPsec client to connect CNet's wireless broadband router CWR-854(F) with VPN capability. The VPN feature can be used for secure remote access to a home or work network from anywhere on the Internet.

**VPN Client Software** used for this test is SSH-Sentinel v1.4 which is free for non-commercial use.



## Applications:



[www.cnetusa.com](http://www.cnetusa.com)

Connect securely to home/work computers over the Internet. You could be at work, at a friend's house or on the road.

**Equipment Needed:**

- 1- A solid broadband connection to the Internet at home or work where CWR-854 is used. CWR-854 needs to be configured for IPsec VPN capability
- 2- A client system with a VPN client software. We used SSH-Sentinel VPN client software ( a trial version is available on the Internet)

**Configuration Overview:**

In the first scenario we will be working with two computers and a CWR-854 VPN router. The assumption is that we are away from home and need to access a computer on the home network connected to CWR-854. The computer we're working from is connected to the Internet through a Cable/DSL modem or we are dialing up using a modem.

In the second scenario, the client system is also behind a NAT route. In this case the computer we're working on is connected to a router and through a Cable/DSL modem to the Internet.

**First Scenario:**

To configure VPN both on the client system as well as the router, we need to know about the IP address schema used on the home network. By default the LAN IP of CWR-854 is 192.168.1.254. Computers that are be accessed from the Internet are better to have a fixed IP address assigned to them. Below are what we need to know:

Home WAN IP address (this is the WAN IP of the VPN router CWR-854 used at home or work) for example: 204.30.90.120

Home LAN IP address: (Default LAN IP of CWR-854 is 192.168.1.254)

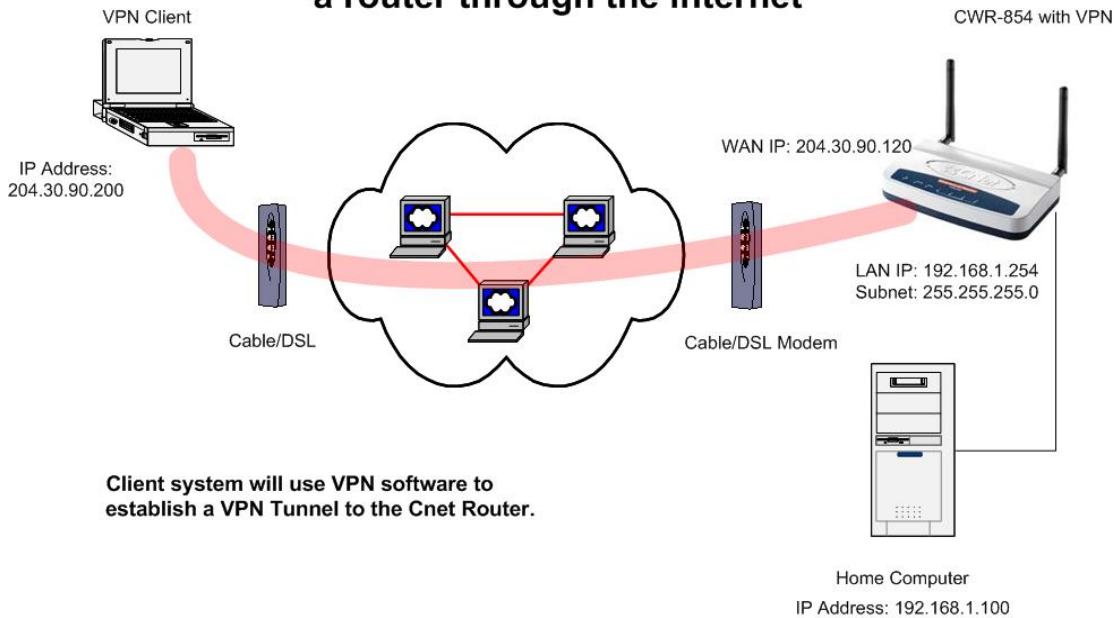
Home LAN IP Network : (Default is 192.168.1.0, Subnet 255.255.255.0)

Computer to be accessed on the home network: 192.168.1.100

VPN Client (remote) computer on the Internet for example: 204.30.90.200



## VPN setup between a client and a router through the Internet



### Router's VPN Configuration:

Please use the routers' default IP address 192.168.1.254 to access its configuration.

VPN Setup

This page is used to enable/disable VPN function and select a VPN connection to edit/delete.

Enable IPSec VPN     Enable NAT Traversal   

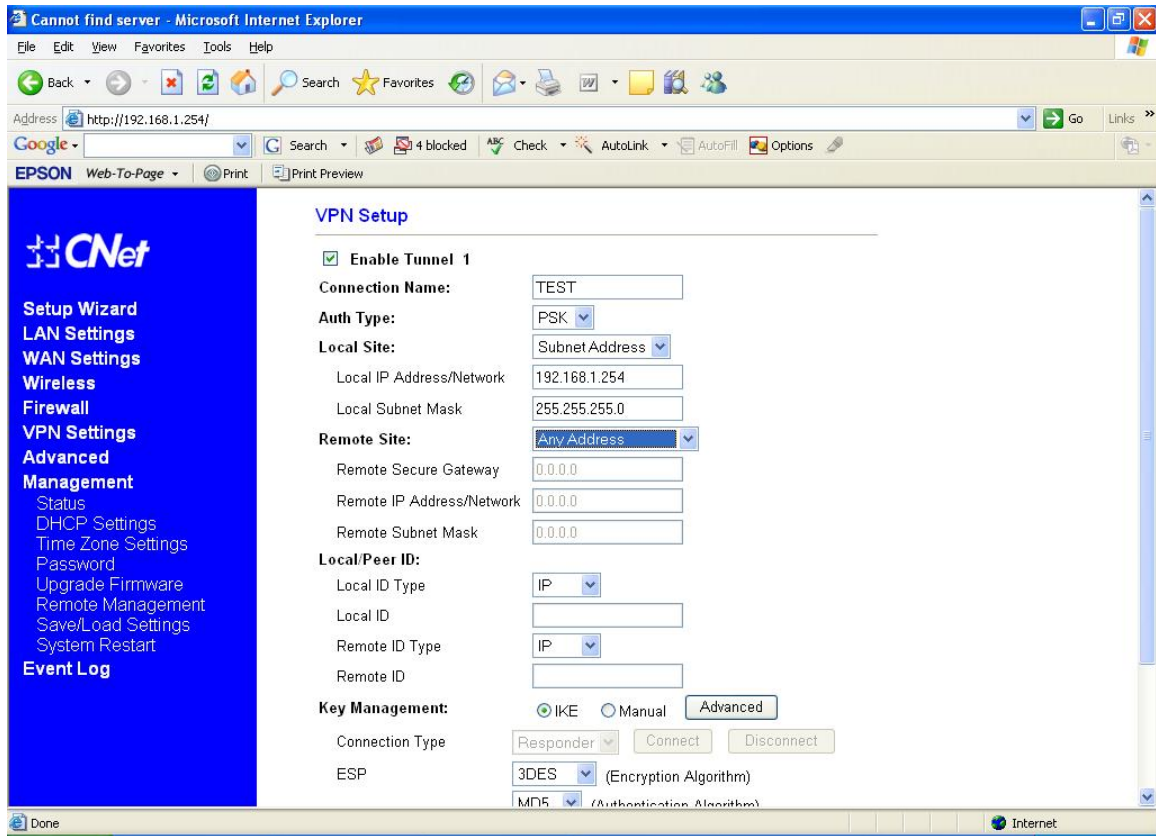
Current VPN Connection Table:    WAN IP:0.0.0.0

#	Name	Active	Local Address	Remote Address	Remote Gateway	Status
1	-	-	-	-	-	-
2	-	-	-	-	-	-
3	-	-	-	-	-	-
4	-	-	-	-	-	-
5	-	-	-	-	-	-
6	-	-	-	-	-	-
7	-	-	-	-	-	-
8	-	-	-	-	-	-
9	-	-	-	-	-	-
10	-	-	-	-	-	-

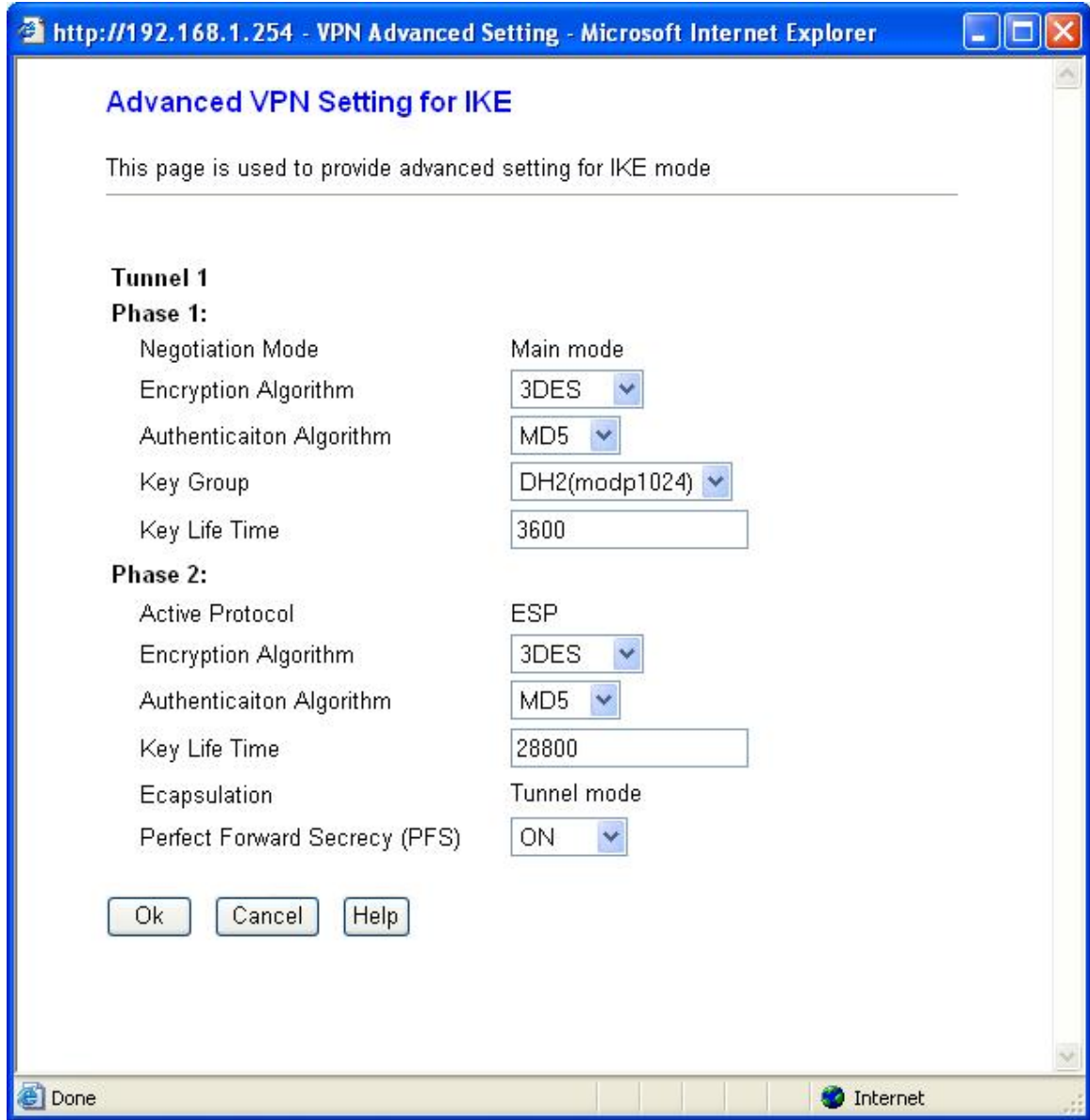


As shown above, CWR-854 can store 10 different VPN profiles. We need to enable IPSec VPN and then click on edit to configure the first profile.



- Use any name for the connection.
- Authentication will be through the Pre-Shared Key (PSK). Basically anyone who wants to have VPN connectivity to the router needs to have this key. We will later on use this same key in the client configuration.
- The next step is to enter the IP information for Local and remote sites. For local site choose “Subnet Address” to allow access to the whole LAN network. For remote site, choose “Any Address” so that the router accepts VPN requests from any IP address.
- Both local and remote systems are identified by IP.
- Key management is auto (IKE). Click the advance key to see the settings for phase 1 and 2 negotiations. In phase 1 peers are authenticated to each other and a secure encrypted link is established to start phase 2 which is the actual negotiation of security services for the IPSec-compliant VPN channel. As you can see in the next image, 3DES and MD5 are the chosen encryption and authentication methods and for additional security PFS (Perfect Forward Secrecy) is also selected.





The last step to finalize VPN configuration is to enter the PSK (Pre-Shared Key) and save settings. The router is now ready to accept incoming VPN connections.




Cannot find server - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://192.168.1.254/

Google Search 4 blocked ABC Check AutoLink AutoFill Options

EPSON Web-To-Page Print Print Preview



Setup Wizard  
LAN Settings  
WAN Settings  
Wireless  
Firewall  
VPN Settings  
Advanced  
Management  
Status  
DHCP Settings  
Time Zone Settings  
Password  
Upgrade Firmware  
Remote Management  
Save/Load Settings  
System Restart  
Event Log

Local IP Address/Network: 192.168.1.254

Local Subnet Mask: 255.255.255.0

**Remote Site:** Any Address

Remote Secure Gateway: 0.0.0.0

Remote IP Address/Network: 0.0.0.0

Remote Subnet Mask: 0.0.0.0

**Local/Peer ID:**

Local ID Type: IP

Local ID:

Remote ID Type: IP

Remote ID:

**Key Management:**  IKE  Manual

Connection Type: Responder

ESP: 3DES (Encryption Algorithm)

MD5 (Authentication Algorithm)

PreShared Key: 1234567890

Remote RSA Key:

Status: Disconnected


Wireless-G Router - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://192.168.1.254/home.asp

Google Search 4 blocked ABC Check AutoLink AutoFill Options

EPSON Web-To-Page Print Print Preview



Setup Wizard  
LAN Settings  
WAN Settings  
Wireless  
Firewall  
VPN Settings  
Advanced  
Management  
Event Log

### VPN Setup

This page is used to enable/disable VPN function and select a VPN connection to edit/delete.

Enable IPSec VPN  Enable NAT Traversal

Current VPN Connection Table: WAN IP:192.168.0.254

#	Name	Active	Local Address	Remote Address	Remote Gateway	Status
1	test	Y	192.168.1.0/24	Any	Any	Disconnected
2	-	-	-	-	-	-
3	-	-	-	-	-	-
4	-	-	-	-	-	-
5	-	-	-	-	-	-
6	-	-	-	-	-	-
7	-	-	-	-	-	-
8	-	-	-	-	-	-
9	-	-	-	-	-	-
10	-	-	-	-	-	-



## Second Scenario:

In this scenario the remote system is behind a NAT router for example another CWR-854. The connection is from VPN client >> NAT router>> Cable/DSL modem >> Internet >>Cable/DSL modem >>VPN router.

The only difference in the configuration with scenario one is to configure the VPN router's remote site to be "NAT-T any address" as below picture shows:

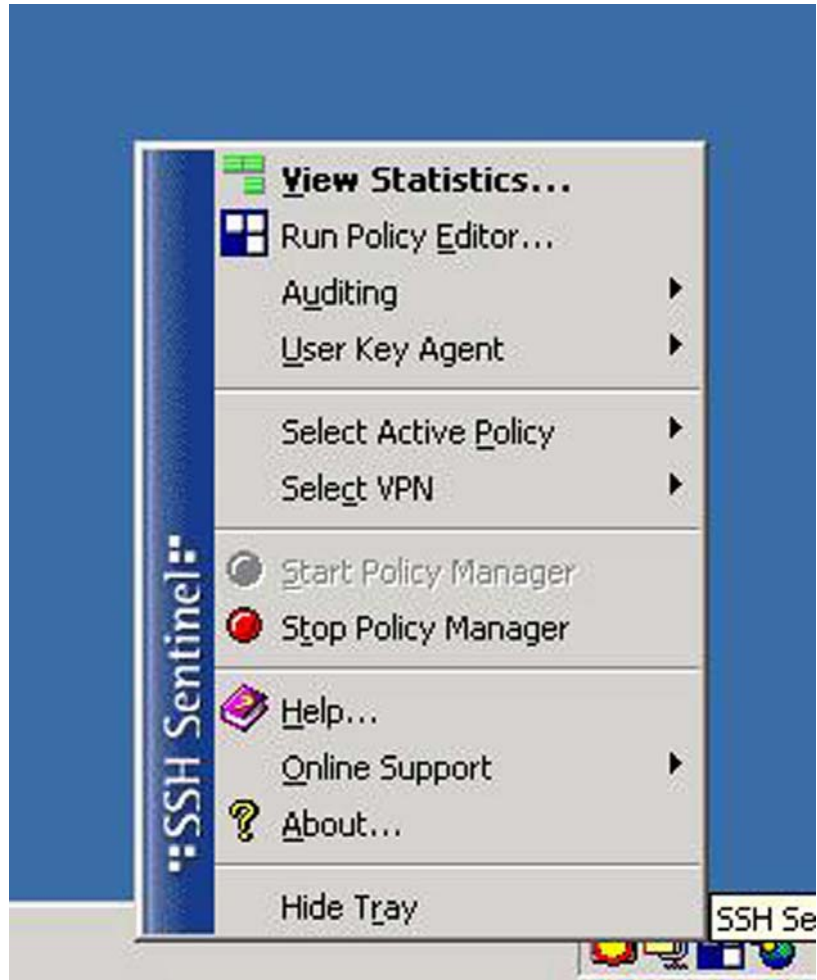
The screenshot shows the configuration page for a Wireless-G Router. The browser window is titled "Wireless-G Router - Microsoft Internet Explorer" and the address bar shows "http://192.168.1.254/home.asp". The page content includes a navigation menu on the left with options like "Setup Wizard", "LAN Settings", "WAN Settings", "Wireless", "Firewall", "VPN Settings", "Advanced", "Management", and "Event Log". The main configuration area is divided into several sections: "Local IP Address/Network" (192.168.1.254), "Local Subnet Mask" (255.255.255.0), "Remote Site" (NAT-T Any Address), "Remote Secure Gateway" (0.0.0.0), "Remote IP Address/Network" (204.30.90.0), "Remote Subnet Mask" (255.255.255.0), "Local/Peer ID" (Local ID Type: IP, Remote ID Type: IP), and "Key Management" (IKE selected, Connection Type: Responder, ESP: 3DES, Authentication Algorithm: MD5, PreShared Key: 1234567890). The status is "Disconnected". Buttons for "Apply Changes", "Reset", "Refresh", "Back", and "Help" are located at the bottom of the configuration area.



## VPN Client Configuration

The client software used for this test is SSH-Sentinel v1.4.

The SSH Sentinel software is configured in two steps. The first one involves the creation of a key management and the second one is the actual VPN security policy. After the software is installed, right click on the Sentinel icon in the task bar and select “Run Policy Editor”.



### Configuring SSH Sentinel Key Management

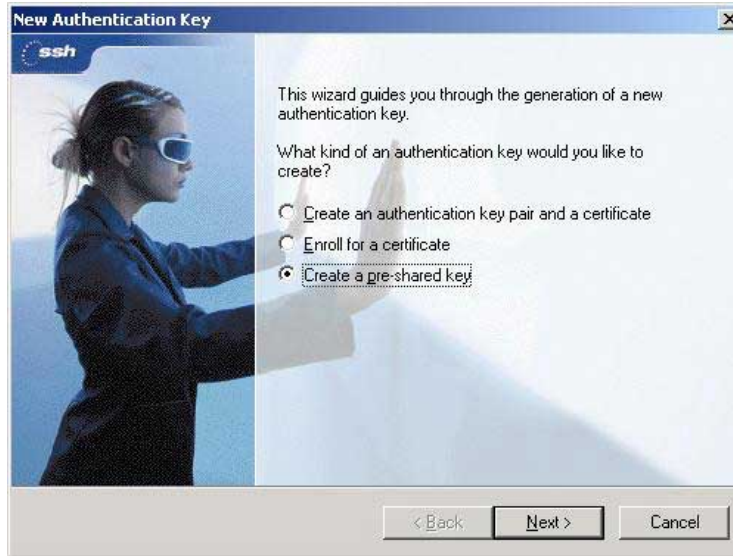
From the SSH Sentinel policy editor, click on “Key Management” tab. Then select the add button under “My Keys” folder.







From the “New Authentication Key” window, select the “create a pre-shared key” radio button and click next.



In the next window, type a name and the same exact key you have entered in the router's VPN configuration and click "Finish".

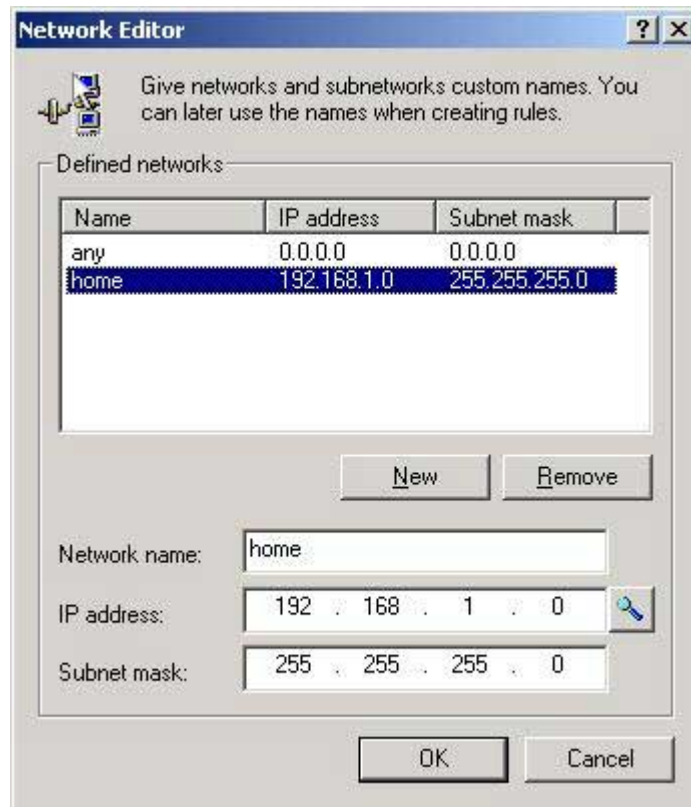


## Configuring SSH Sentinel Security Policy

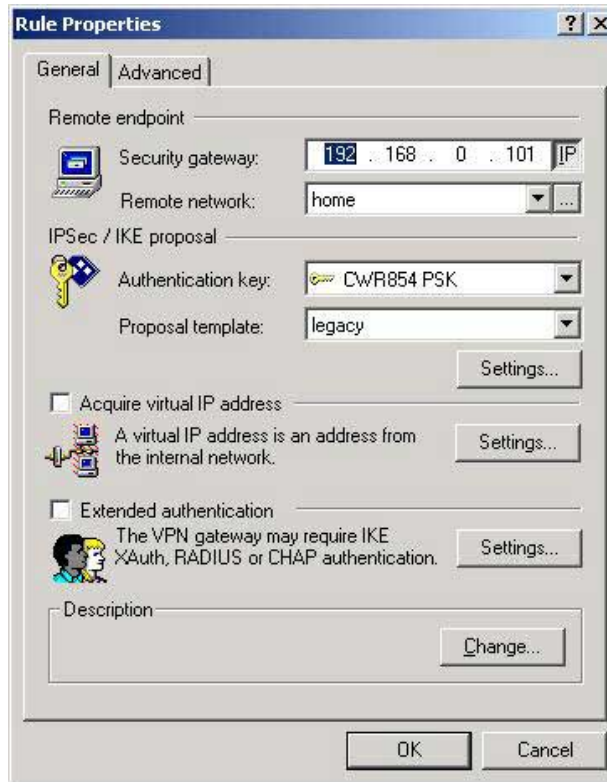
From the Security Policy window, click on the “Security Policy” tab, select VPN connections and click on “Add” button.



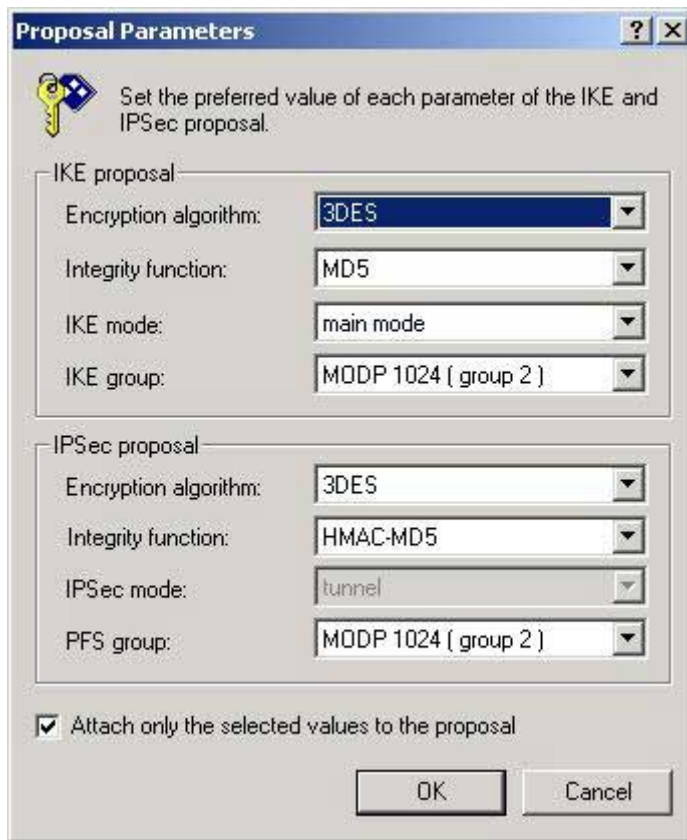
In the “Add VPN Connection” window, enter an IP address or a Domain Name associated with the WAN IP of the CNet router. For remote network, click the “...” micro button and enter the remote network information. The default LAN network address of CWR-854 is 192.168.1.0 with 255.255.255.0 for subnet mask.



Click OK to save the changes and return to the “Rule Properties” window.



Click on the IPSec/IKE proposal settings button to view proposal parameters.



Click OK to go back to “Rule Properties” window. Click on the Advanced tab to view Security association lifetimes as well as Audit and some other advanced settings.

If the VPN client system is sitting behind a NAT device, you’ll need to check the box next to “Pass NAT device” using NAT-T.





At this stage we've completed SSH Sentinel configuration and we are ready to perform a diagnostic test. Click OK to go back to the SSH Sentinel Policy Editor window and click "Apply" to update security policy changes we've made.

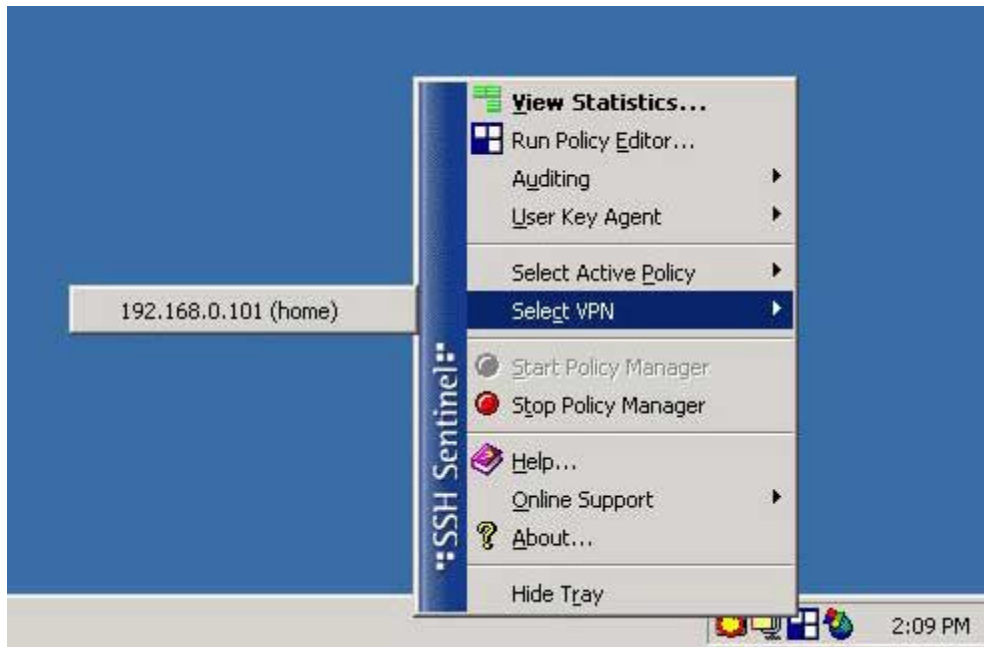
Now click on "Diagnostics" to start probing the connection to the VPN server. If Diagnostics complete successfully, it means that you can establish an IPSec protected connection to the VPN server.



We can now use the SSH Sentinel icon in the task bar, select the VPN server and establish the VPN tunnel.







### Testing VPN Connection

To test the VPN connection, bring up a DOS window and try a ping to the IP address of one of the computers at home. If ping is successful then the connection is established and you should be able to see and map network drives to systems behind the VPN router.



[www.cnetusa.com](http://www.cnetusa.com)